

Customer No. 24498
Attorney Docket No. PU030342
Office Action Date: September 10, 2008

REMARKS

This application has been reviewed in light of the Office Action dated September 10, 2008. Claims 1-13 are currently pending and stand rejected. No new matter has been added. Reconsideration of the claim rejections is requested in view of the above claim amendments and following remarks.

Responsive to the objection to the specification applicants have attached the abstract, reproduced on a single sheet. Responsive to the objection to the drawings, applicants submit corrected drawings; wherein the label "Substitute Sheet" has been deleted.

Rejections under 35 U.S.C. 102 (e)

Claims 1, 4-6, 8-10 and 13 are rejected under 35 U.S.C. 102 (e) as being anticipated by Marsh (U.S. Patent No. 7,080,039). Applicants respectfully assert that for the reasons discussed below claims 1, 6, 8-10 and 13, are not anticipated Marsh.

Marsh is directed to systems and methods for associating media content with households using smart cards. Marsh teaches using household identifiers on smart cards in order to encrypt or decrypt media content. Marsh does not, however, teach or suggest each and every limitation of claims 1, 6, 8-10 and 13 of the present invention. Each claim is discussed below.

Customer No. 24498
Attorney Docket No. PU030342
Office Action Date: September 10, 2008

Claim 1

Marsh fails to disclose or remotely suggest "a removable digital memory including a port at which digital information stored on said memory can be accessed," as recited in claim 1.

Marsh teaches a system that can receive, store, transmit over a network, and render media content (see col. 13, lines 29-31). Marsh discloses numerous devices and modules that may be part of or connected to the system in Figs. 2-3 and col. 4-8. However, nowhere in this detailed, in-depth description does Marsh suggest "a removable digital memory including a port at which digital information stored on said memory can be accessed."

Claim 1 of the present invention explicitly recites a removable digital memory. Support for this is found in Figs. 1-5 of the present specification, which clearly show a removable memory (a hard disk drive) connected to the system, and paragraph [0008] which discusses the removable mass memory device.

Column 7, lines 11-25 of Marsh, as cited by the Examiner, does not teach the removable digital memory claimed in claim 1. The cited section of Marsh describes coupling a set-top box, which receives the media via cable or other transmission, to the system. Marsh does not suggest that the set-top box is a removable digital memory device, nor would one skilled in the art interpret a set-top box as such. Further, one skilled in the art would certainly interpret the "source device" of the present invention as being a set-top box or other similar device. Thus, the set-top box disclosed by Marsh may be, arguendo, analogous to the source device in the present invention. As such, the set-top box could not be considered a device that is external and removable from the source device because it is, for all intents and

Customer No. 24498
Attorney Docket No. PU030342
Office Action Date: September 10, 2008

purposes, the source device itself. Therefore, it is clear that Marsh does not teach “a removable digital memory including a port at which digital information stored on said memory can be accessed,” as claimed in claim 1.

Furthermore, Marsh does not teach or suggest a device comprising, inter alia, “memory for storing first conditional access data and at least one content encryption key,” as recited in claim 1. The Examiner contends that column 9, lines 57-67 of Marsh teaches this element. The applicants disagree.

The section of Marsh cited by the Examiner discusses the authentication process of a certificate, not memory on a device for storing conditional access data and encryption key(s). Moreover, column 9 of Marsh provides detailed explanation of Fig. 4 which depicts the components of the smart card. Thus, the certificate and public keys referred to in column 9, lines 57-67 of Marsh describe information stored on the smart card, not memory on the device into which the smart card is inserted, as claimed in claim 1.

The only portion of the cited section that even hints at anything resembling memory is col. 9, lines 64-65 where Marsh describes that the encrypting module of the device into which the smart card is inserted “know[s] the public key of the licensing authority, to verify that the certificate that is presented by smart card was indeed digitally signed by the licensing authority.” First, the word “knowing” does not teach a memory which stores the public key. A system or module may “know” something through its connection to another device, system, or module. Thus, “knowing the public key of the licensing authority, to verify ... the certificate,” does not teach or suggest a device comprising, inter alia, “memory for storing first conditional access data and at least one content encryption key.”

Customer No. 24498
Attorney Docket No. PU030342
Office Action Date: September 10, 2008

In addition, this statement does not teach or suggest that a "content encryption key" is stored on the device into which the access card is inserted, as essentially claimed in claim 1. The public key stored on the device in Marsh, described in col. 9, lines 64-65, has nothing to do with the encryption or decryption of the media content. Rather, it's only purpose is to verify the certificate presented by the smart card. Thus, while this may be a public key, it is not a "content encryption key." Furthermore, it is quite clear from Fig. 4 and column 9, lines 9-20 of Marsh that all of the certificates and content encryption keys in Marsh are stored in memory on the smart card, not on the device into which the smart card is inserted as claimed in claim 1. As such, it is clear that Marsh does not teach or suggest "*memory for storing first conditional access data and at least one content encryption key.*"

Therefore, for at least the foregoing reasons, claim 1 is believed to be patentable over Marsh.

Claim 6

Marsh does not teach or suggest an access card comprising, inter alia, "*memory, [which] following authentication of said card with a destination device, [is] updated to store a public key of a public/private key pair stored in said destination device,*" as recited in claim 6.

As discussed above, the content encryption keys in Marsh are originally stored in memory on the smart card, not on the device into which the smart card is inserted. Thus, there is no need for Marsh to update the access card's memory to store a key originally stored on a device. Further, Marsh makes no mention of updating the key(s) on the smart card at all.

In the present invention, however, the access card does not originally include the encryption keys. These keys are loaded onto the card from the destination and source

Customer No. 24498
Attorney Docket No. PU030342
Office Action Date: September 10, 2008

devices of the media. Claim 6 further recites that the media content is then encrypted using the keys from both the destination and source devices. This provides increased security because only the destination device can decrypt the media on the removable storage.

Marsh does not teach or suggest an access card that is authenticated with the destination device as part of the encryption process of the media. The only time Marsh alludes to a destination device is in discussing that the "decryption and rendering [of the media content] can be performed by any system to which smart card is in communication (e.g. plugged into)" (col. 14, lines 19-23). However, at this point, the media has already been encrypted. Thus, it is quite clear that there is no key from the destination device stored on the access card in order to encrypt the media. Moreover, it is clear from Marsh's disclosure that the media can be decrypted by "any system" that Marsh does not contemplate the increased level of security provided by the present invention.

Therefore, for at least the foregoing reasons, Marsh does not teach or suggest claim 6 for the at least the above reasons.

Claim 8

Marsh does not disclose or suggest a digital information destination device comprising, inter alia, "memory preloaded with at least a second stored User Certificate and mutually corresponding private and public encryption keys associated with said destination device," as recited in claim 8.

The Examiner cites Fig. 4 of Marsh as teaching this element. As mentioned above with respect to claim 1, Fig. 4 depicts the smart card used in Marsh; it does not depict or have anything to do with the memory of the digital information destination device. Moreover, column 9, lines 9-20 of Marsh make clear that all of the content encryption keys in

Customer No. 24498
Attorney Docket No. PU030342
Office Action Date: September 10, 2008

Marsh are originally stored in memory on the smart card, not on the device into which the smart card is inserted. Furthermore, Marsh discloses that the media can be encrypted without a smart card even divulging the encryption key to and device (col. 9, lines 33-35). Therefore, it is very clear that Marsh does not teach or remotely suggest a digital information destination device comprising "memory preloaded with corresponding private and public encryption keys associated with said destination device." As a result, claim 8 is believed to be patentable over Marsh for at least the above-mentioned reasons.

Claim 9

For the reasons discussed above with reference to claim 1, it is clear that Marsh fails to teach or suggest a "source device having a removable digital memory containing information accessible to the source device," as recited in the preamble of claim 9, and a method "encrypting said information stored in said removable digital memory using at least one content encryption key stored in said source device," as recited in the body of claim 9. Please refer to the remarks for claim 1.

Claim 10

For at least the reasons discussed above with reference to claim 1, it is clear that Marsh fails to disclose or suggest "providing a source device having a removable digital memory," as recited in claim 10.

Moreover, Marsh does not teach or suggest that the source device "includes a first Conditional Access Certificate" nor does Marsh suggest "providing a destination device having a second stored User Certificate" and also including mutually corresponding private and public encryption keys associated with said destination device." As discussed above, it is clear from Fig. 4 and col. 9, lines 9-20 of Marsh that, in Marsh, it is the smart

Customer No. 24498
Attorney Docket No. PU030342
Office Action Date: September 10, 2008

card that holds the user certificates and encryption keys, not the destination and source devices.

In addition, Marsh does not teach or suggest a method which includes "placing [the] access card in said access card port of said destination device" for authentication and "writing said public encryption key from said destination device to said access card" prior to placing the access card in the source device of the media.

Marsh only describes authenticating the access card in the source device (see e.g. col. 10, lines 22-43). When doing so, there is not even the slightest suggestion that the card had been already authenticated with the destination device or that an encryption key on the card originated from the destination device. In fact, as discussed above in reference to claim 8, it is clear that the encryption keys in Marsh originate from the access card itself.

Furthermore, as discussed with reference to claim 6, the steps of authenticating the access card with the destination device and transferring an encryption key from the destination device to the access card before inserting the card into the source device provides enhanced security that are not contemplated by Marsh. Thus, Marsh clearly does not teach or suggest claim 10. As such, claim 10 is believed to be patentable over Marsh.

Claim 13

Marsh does not disclose or suggest an "access card comprising: a memory having at various times at least first, second, and third states...", as recited in claim 13.

The present invention, however, particularly describes that the information stored in the memory of the access card changes throughout the encryption and decryption process. As discussed above with reference to claim 6, both the destination device and the source device write encryption keys to the memory of the access card during the process. The addition of

Customer No. 24498
Attorney Docket No. PU030342
Office Action Date: September 10, 2008

these keys to the memory of the access card is what creates the different states referred to in claim 13.

Further, Figs. 1-5 of the present invention clearly demonstrate the different states recited in claim 13 by particularly showing the different information stored on the access card at different times during the encryption and decryption process. For example, Fig. 1 shows the first state, where the access card's memory holds CA Certificate A and User Certificate B; Figs. 2-3 show the second state, where the access card's memory holds CA Certificate A, User Certificate B and Public Key Encryption Key; and Figs. 4-5 shows the third state, with the access card's memory holding CA Certificate A, User Certificate B, Public Key Encryption Key and Encrypted Content Encryption Keys.

As mentioned earlier in reference to claim 6, Marsh does not make any suggestion that any information on the smart card is changed and/or updated. In fact, Marsh strongly implies that the smart card information is static in Fig. 4 and throughout the specification. If the information on the smart card remains static, it is impossible for the memory on the smart card to have, at various times, three different states. It is well known in the art that a smart card whose memory does not change has only one, static state.

The portion of Marsh cited by the Examiner (col. 7, lines 11-25) describes the scrambling of the content passed from the set-top box to the encryption module of Marsh's system. It does not even mention an access card at all. Furthermore, it does not disclose any different states of any memory defined by the presence of different certificates and encryption keys in the memory. Thus, it is clear that Marsh does not disclose or suggest the access card having various states claimed in claim 13.

Customer No. 24498
Attorney Docket No. PU030342
Office Action Date: September 10, 2008

Since, Marsh fails to teach or suggest all of the aspects of claims 1, 6, 8-10 and 13, these claims are believed to be distinct and patentable over Marsh. Accordingly, Applicants assert that claims 1, 6, 8-10 and 13 are in condition for allowance for at least the stated reasons. Additionally, applicants respectfully assert that claims 4-5 are patentable over Marsh at the very least by their dependence from claim 1. Reconsideration of the rejections is earnestly solicited.

Rejections under 35 U.S.C. 103 (a)

Claims 2, 3, 7, 11 and 12 are rejected under 35 U.S.C. 103 (a) as being unpatentable over Marsh in view of Roskind (U.S. Patent Publication 2003/00466544). Since claims 2, 3, 7, 11 and 12 depend from claims 1, 6 and 10, applicants assert that these claims are patentable over Marsh for at least the same reasons described above.

Roskind does not cure the deficiencies of Marsh in this regard. Roskind is directed to a digital certificate with a limited useful life. Roskind does not disclose systems and methods for encryption and decryption of media content, as claimed in the claims of the present invention. Roskind only teaches systems and methods for authentication of certificates. As such Roskind does not remotely suggest any of the above deficiencies of Marsh. Therefore, the claims of the present invention are believed to be patentable over the combination of Marsh and Roskind. Reconsideration of the obviousness rejection is requested.

Since the cited art fails to disclose or suggest all of the features of independent claims 1, 6, 8-10 and 13, these claims are believed to be distinct and patentable over Marsh and Roskind, taken singly or in combination. Accordingly, applicants respectfully assert that the above-mentioned claims are in a position for allowance for at least the stated reasons. Additionally, applicants respectfully assert that claims 2, 3, 7, 11, and 12 are patentable over


Customer No. 24498
Attorney Docket No. PU030342
Office Action Date: September 10, 2008

Marsh and Roskind at least by virtue of their respective dependencies from the
aforementioned independent claims. Reconsideration of the rejections is earnestly solicited.

In view of the foregoing remarks, it is respectfully submitted that all claims
now pending in the application are in condition for allowance. Early and favorable
reconsideration of the case is respectfully requested.

Respectfully submitted,

By:



Paul P. Kiel
Reg. No. 40,677

Date:

11/14/08

THOMSON LICENSING LLC
Patent Operations
P.O. Box 5312
2 Independence Way
Princeton, NJ 08543-5312